Net-Ready Key Performance Parameter

LTC Tom Gaetjen

J6

Agenda

- Set Stage
- IER Approach
- Net Ready Approach
- Net Ready Key Performance Parameter (NR KPP)
  - Net-Centric Operations and Warfare (NCOW) Reference Model
  - Integrated Architectures
  - Key Interface Profiles
  - Information Assurance
- Program migration to the NR KPP (examples)
- NR KPP status
- Complimentary and Corresponding Systems

Revised DODD 5000.1, DODI 5000.2 and DOD 5000.2R - USD-AT&L

DODD 4630.5 & DODI 4630.8 - OASD-NII

Capabilities

CJCSI 3170 (J8)

- Capability Validation Process/Procedures
- ICD, CDD, CPD Format
- NET READY KPP

CJCSI 6212 (J6)

- Interoperability and Supportability Certification and Testing
- Methodology for Net Ready KPP Development /Validation

Acquisition

Information Support Plan (OASD-NII)

Operational/Systems/Technical Architecture Infrastructure Support

Process

Testing

TEMP

Systems specs accurately reflect requirements and acquisition documents

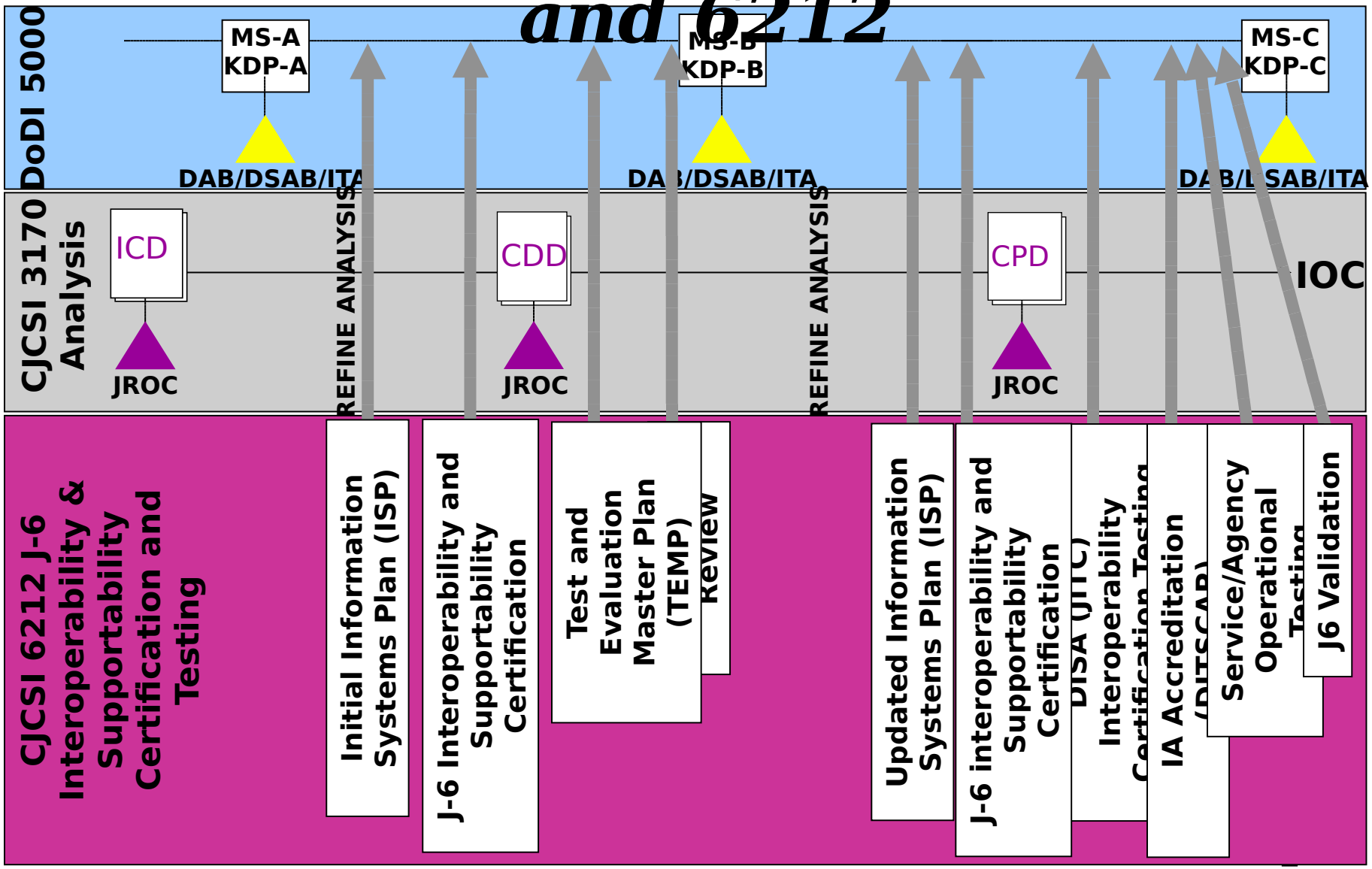
Service/Agency Testing

- DT/Standards Conformance
- OT&E
- Interoperability Testing

DISA(JITC) Interoperability Test Certification

J-6 Interoperability System Validation

Sync – DoDI 5000 &CJCSI 3170 and 6212



Interoperability KPP Today

Top-level IERs will be used as the basis to develop interoperability KPPs. The interoperability KPP definition will include that all top-level IERs will be satisfied to the standards specified in the threshold and objective values.

Typically the threshold criterion for the interoperability KPP will be 100 percent accomplishment of the critical top-level IERs, and the objective criterion for the interoperability KPP will be the accomplishment of all top-level IERs.

Interoperability KPP	Threshold (T)	Objective (O)
All top-level IERs will be satisfied to the standards specified in the Threshold (T) and Objective (O) values.	100% of top-level IERs designated critical	100% of top-level IERs

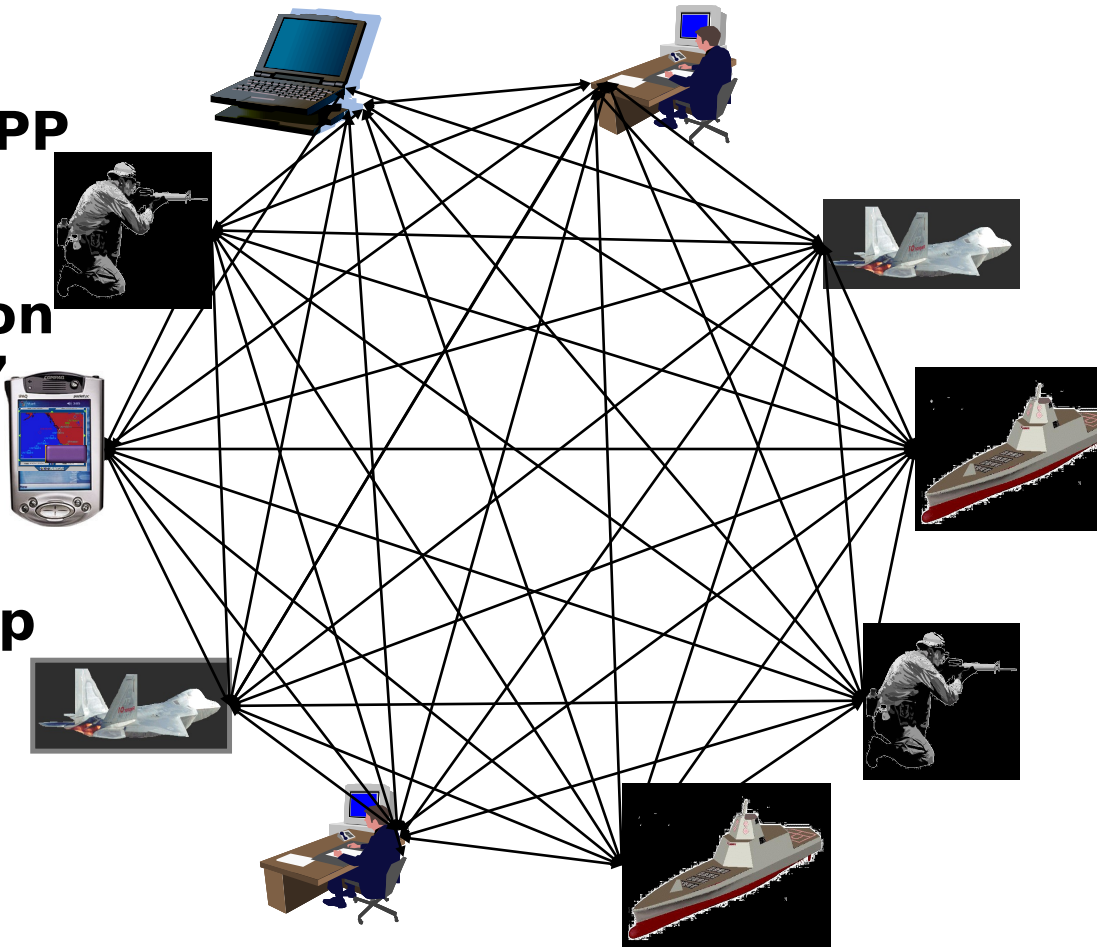
(CJCSI 6212.01B)

Problem: IER Scalability

One-to-One

Current Interoperability KPP centers around one DoD architectural view (OV-3) that contains "Information Exchange Requirements" (IERs)

- **One-to-one relationship (point-to-point)**



This example: 10 systems

IERs 10(9-1) = 90

(OV-3) –Notional USCENTCOM Targeting Extract

* Identifier/ Name of Operational Needline Supported (from OV-2)	* Identifier/ Name of Information Exchange	Nature of Transaction								* Purpose/ Triggering Event	Information Source		Information Destination	
		* Mission/ Scenario	Language (For Multi-National Operations)	* Description (Content)	Size	Units	* Media	Collaborative (Y/N)?	LISI Level Required		* ID of Producing Node (facility or logical node)	* ID/ name of Producing Activity	* ID of Receiving Node (facility or logical node)	* ID/name of Receiving Activity
1	WOC-AOC	Targeting	Eng.	BDA Reports	1-10 pgs	.5-2 MB	.doc .jpg .mpg .ppt .cgm	Y	2a	Air Strike 072200 0615am	XXXth TFW	WOC	609 AIS	AOC
	WOC-AOC	Targeting	Eng.	Target Nominations	1 pg	20KB	.doc	N	1b	ATO XXX 072300	XXXth TFW	WOC	609 AIS	AOC
2														
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
n	MAW-AOC	Targeting	Eng.	BDA Reports	1-10 pgs	.5-2 MB	.doc, .ppt .jpg, .cgm .mpg	Y	2a	Air Strike 072200 0615am	VMF XXX	MAW	609 AIS	AOC

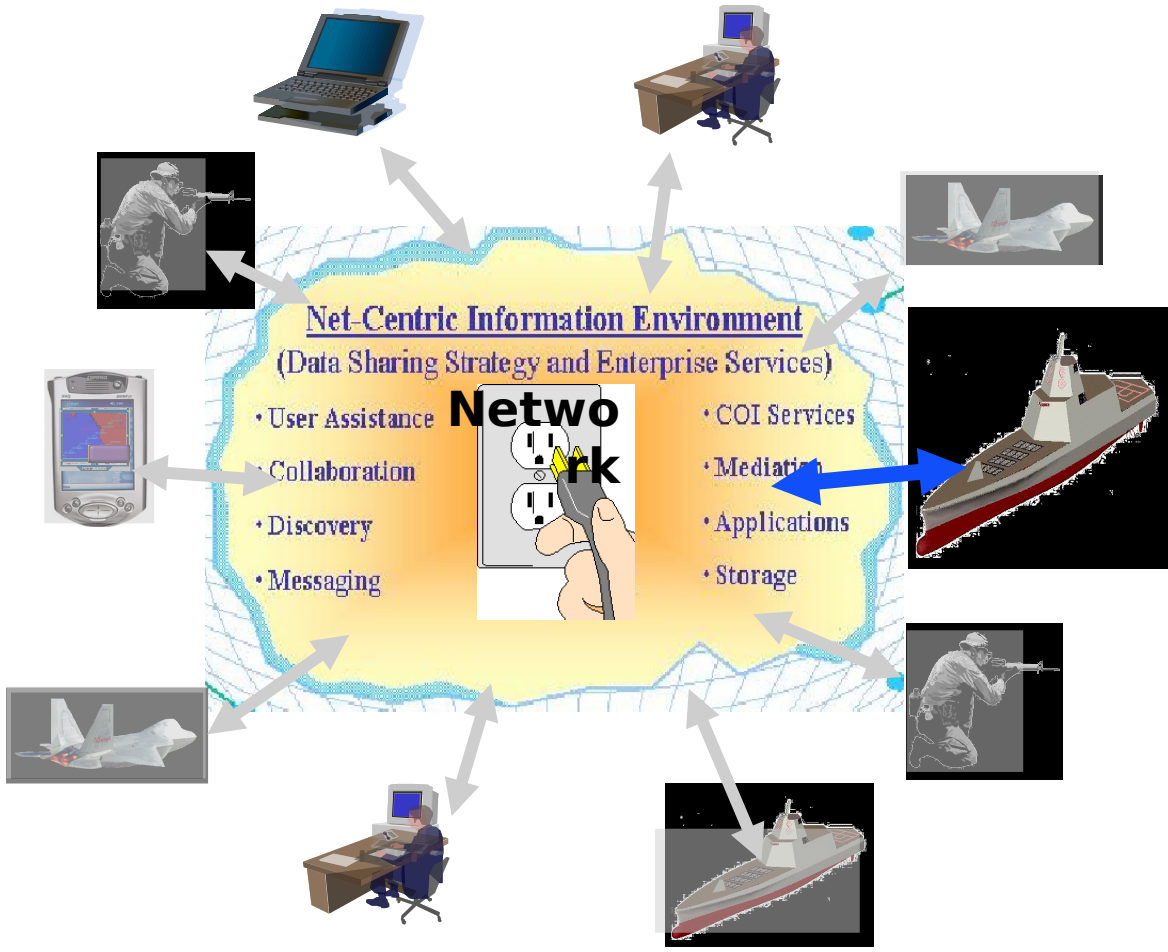
Note: All values shown above are notional.

Solution: The Net-Ready Approach

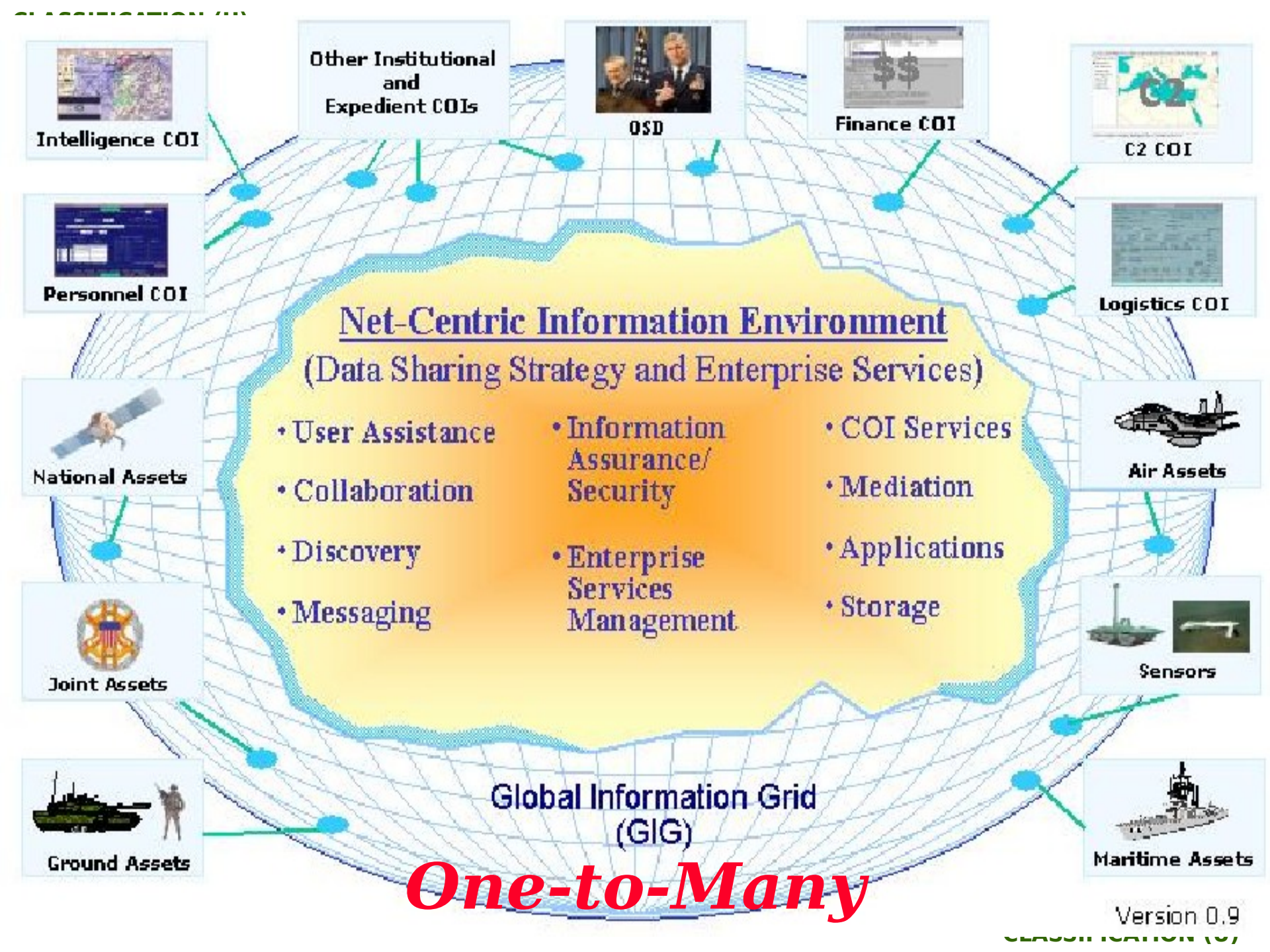
One-to-Many

Net Ready approach centers on central network:

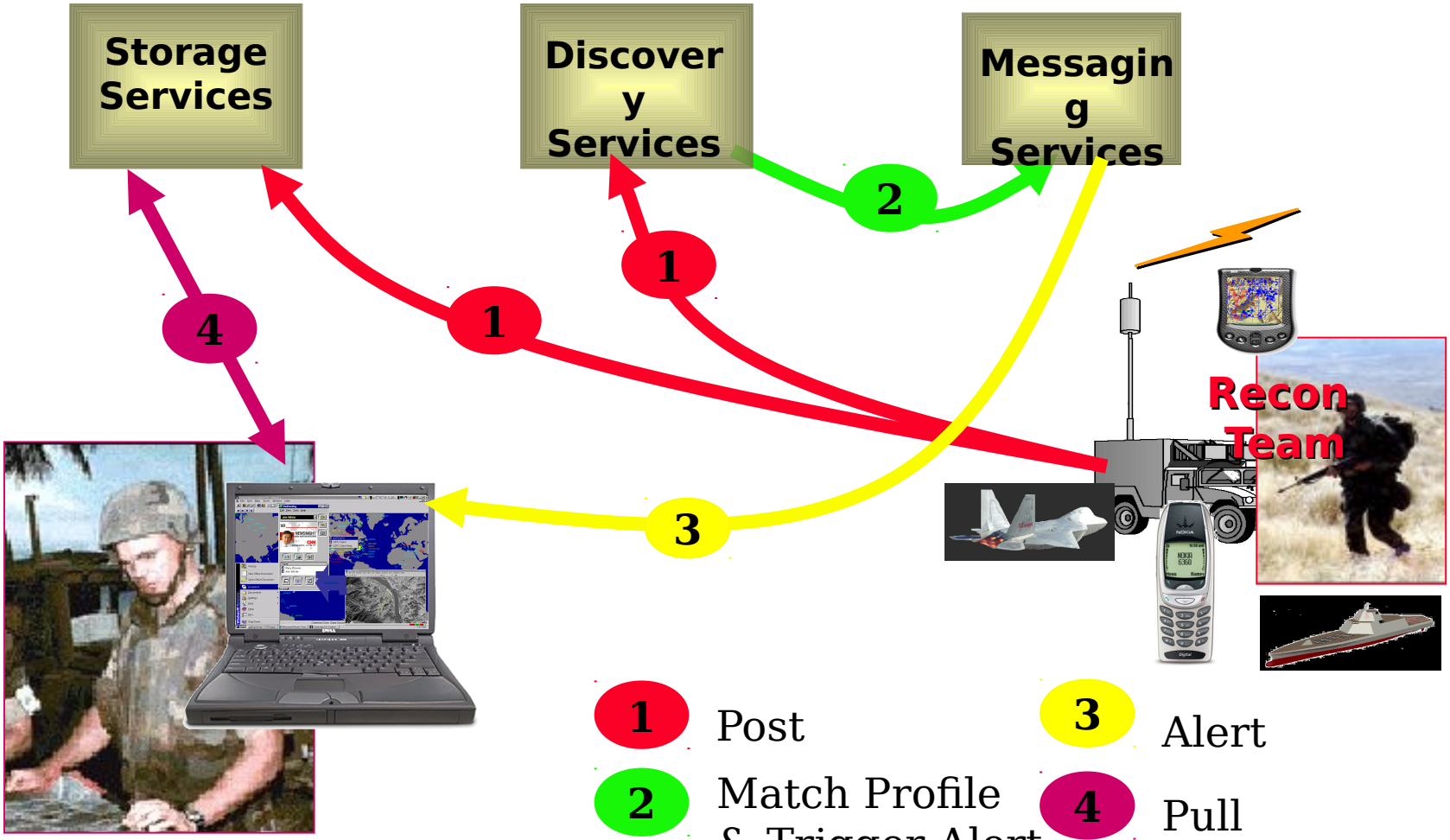
- **Focus on organizational contributions and consumption of information**
- **One-to-network paradigm**



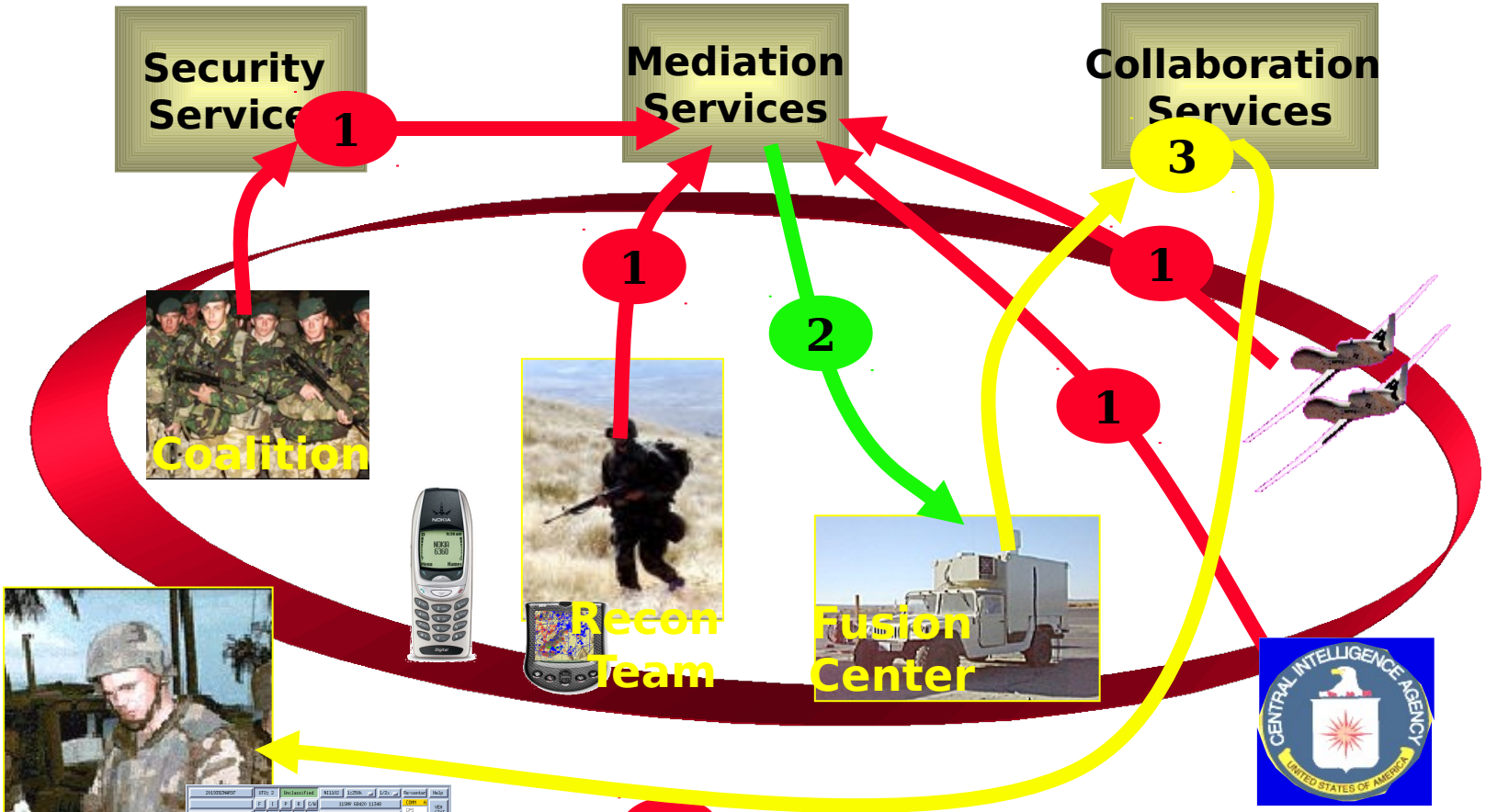
This example: 1 system has to deal 1 interface


Intelligence COI
Other Institutional and Expedient COIs
OSD
Finance COI
C2 COI
Personnel COI
Logistics COI
Net-Centric Information Environment
(Data Sharing Strategy and Enterprise Services)
• User Assistance
• Collaboration
• Discovery
• Messaging
• Information Assurance/ Security
• Enterprise Services Management
• COI Services
• Mediation
• Applications
• Storage
National Assets
Air Assets
Joint Assets
Sensors
Ground Assets
Maritime Assets
Global Information Grid
(GIG)
One-to-Many
Version 0.9

How GES/NCES works



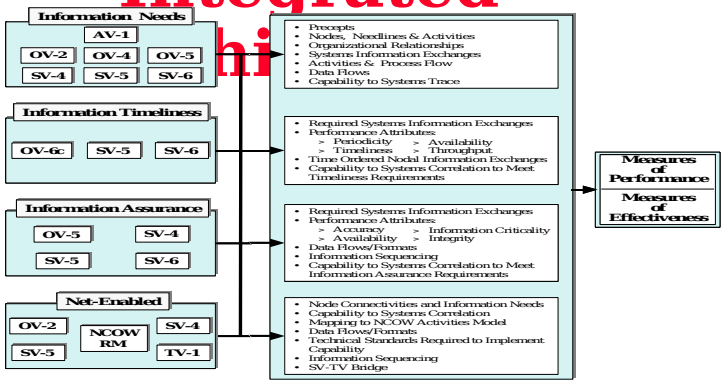
How NCES works (Cont'd)



Net-Ready KPP

NCOW RM Compliance

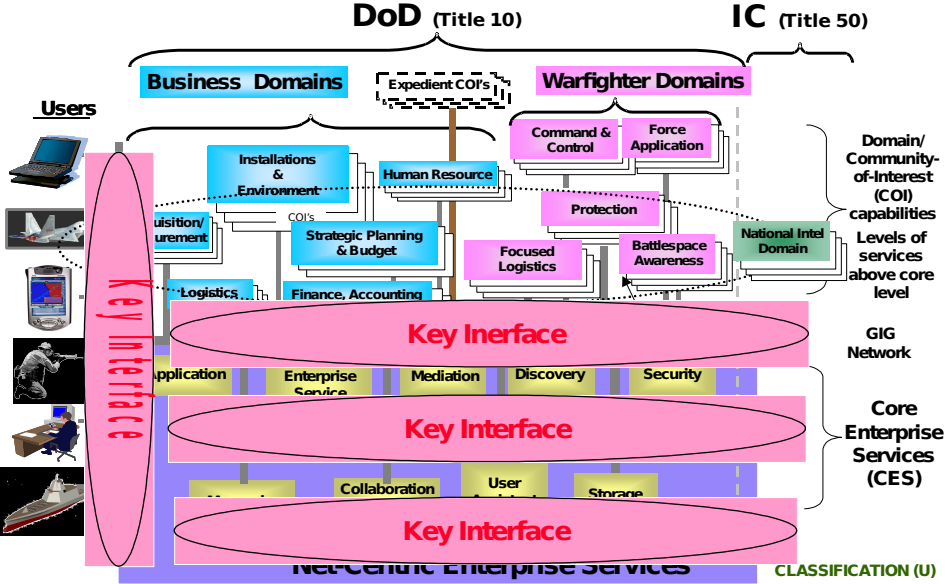
Integrated Architecture



KIP Compliance

CLASSIFICATION (U)

GIG Enterprise Services Vision

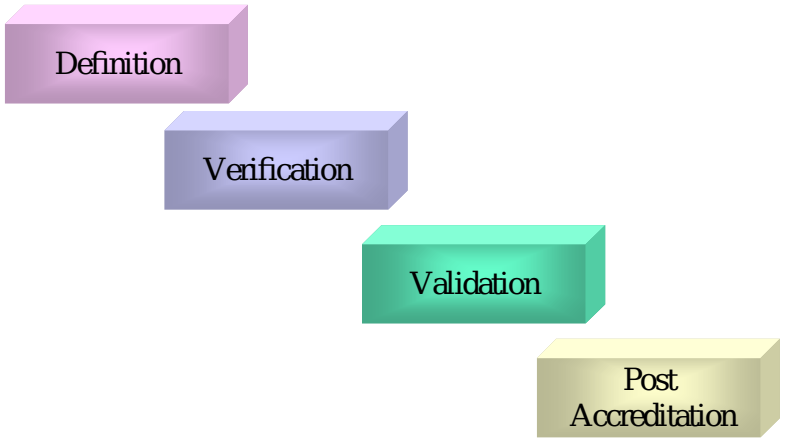


CLASSIFICATION (U)

Information Assurance (DITSCAP*)

CLASSIFICATION (U)

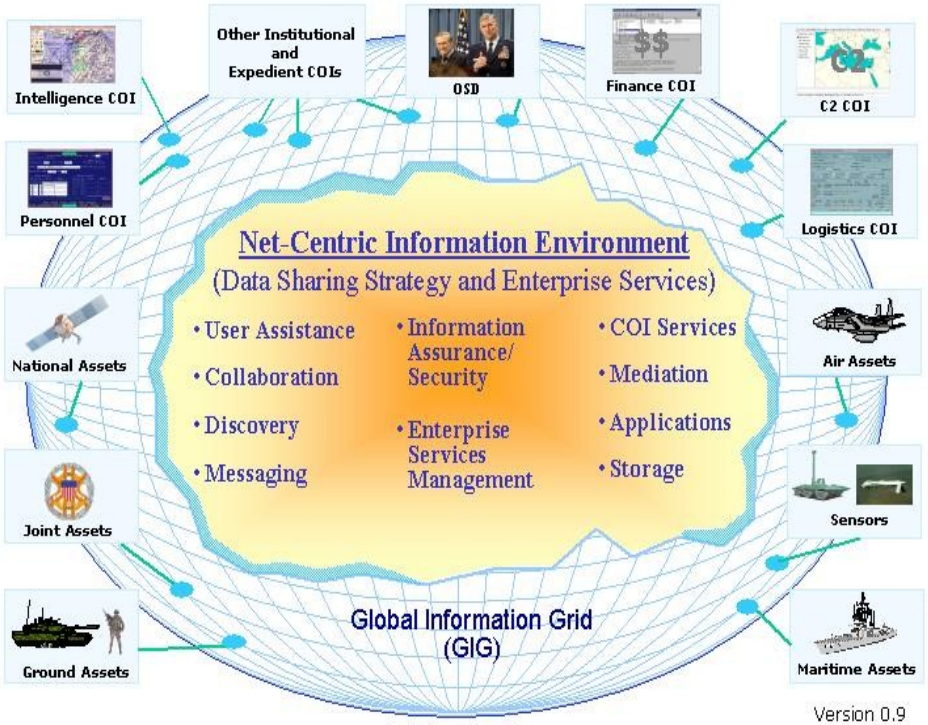
Information Assurance



*DoD Information Technology Security Certification and Accreditation Process

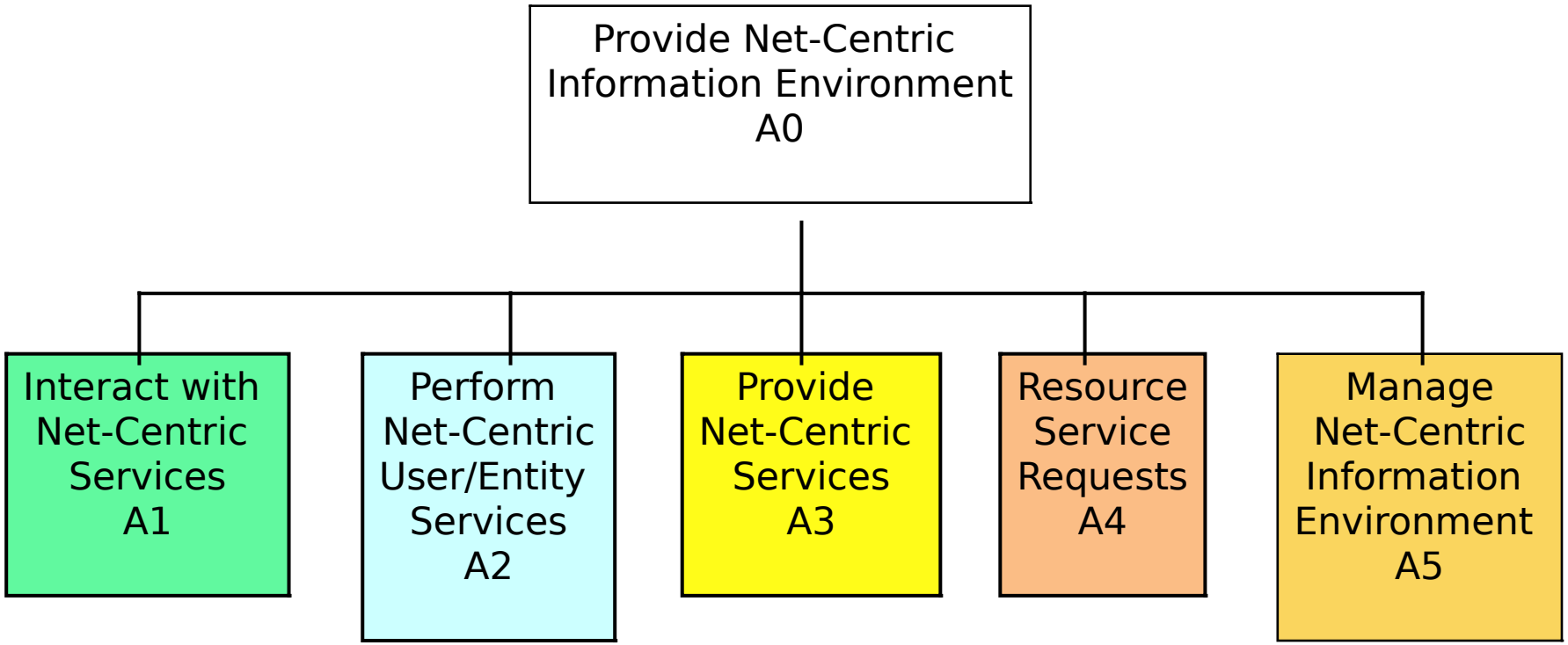
CLASSIFICATION (U)

(NCOW) Reference Model

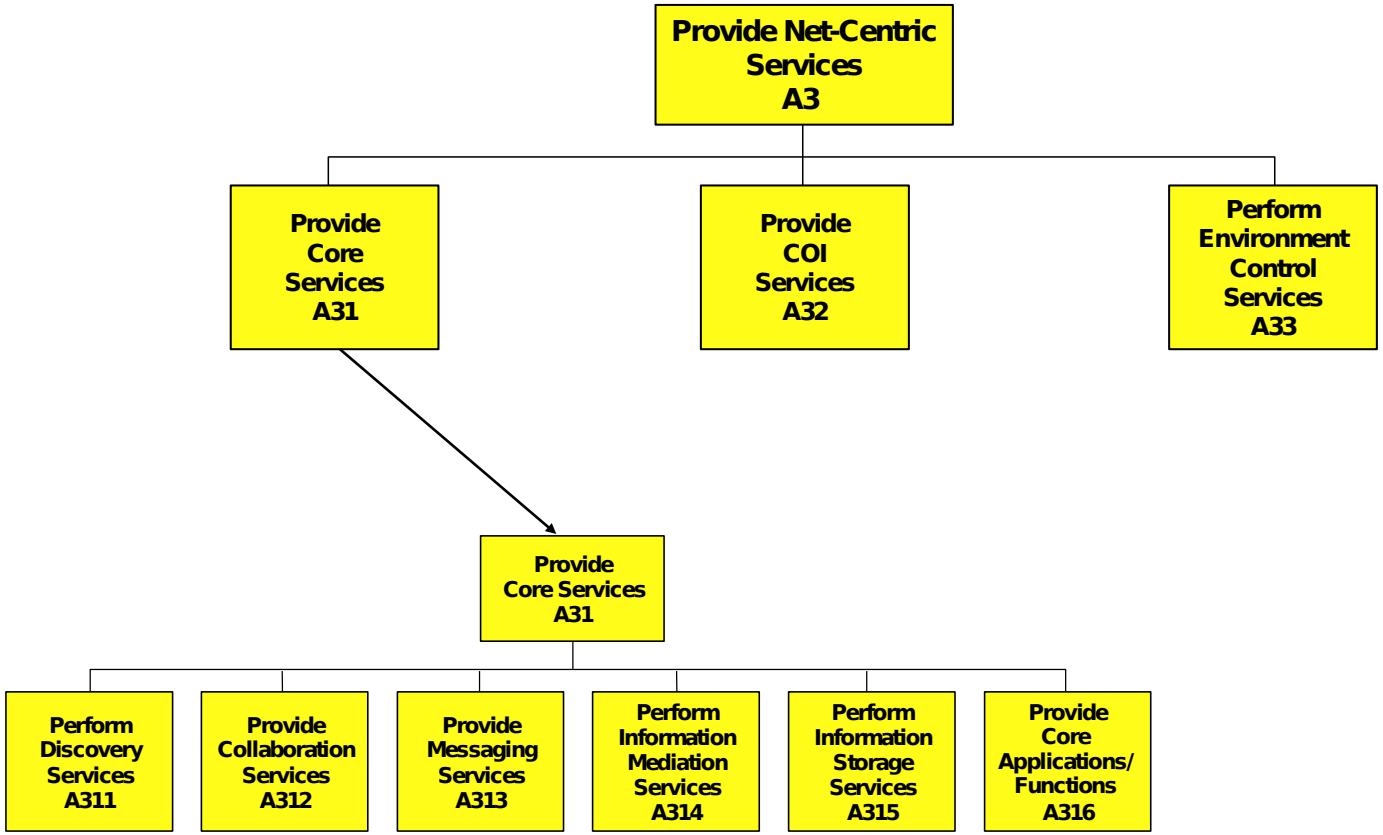


- **Provides a common language and understanding of net-centricity**
- **Specifies the core capabilities of a net-centric DoD architecture**
- **Provides basic templates and guidance for building net-centric DoD architectures**
- **Specifies compliance criteria for measuring and analyzing net-centricity in a DoD architecture.**

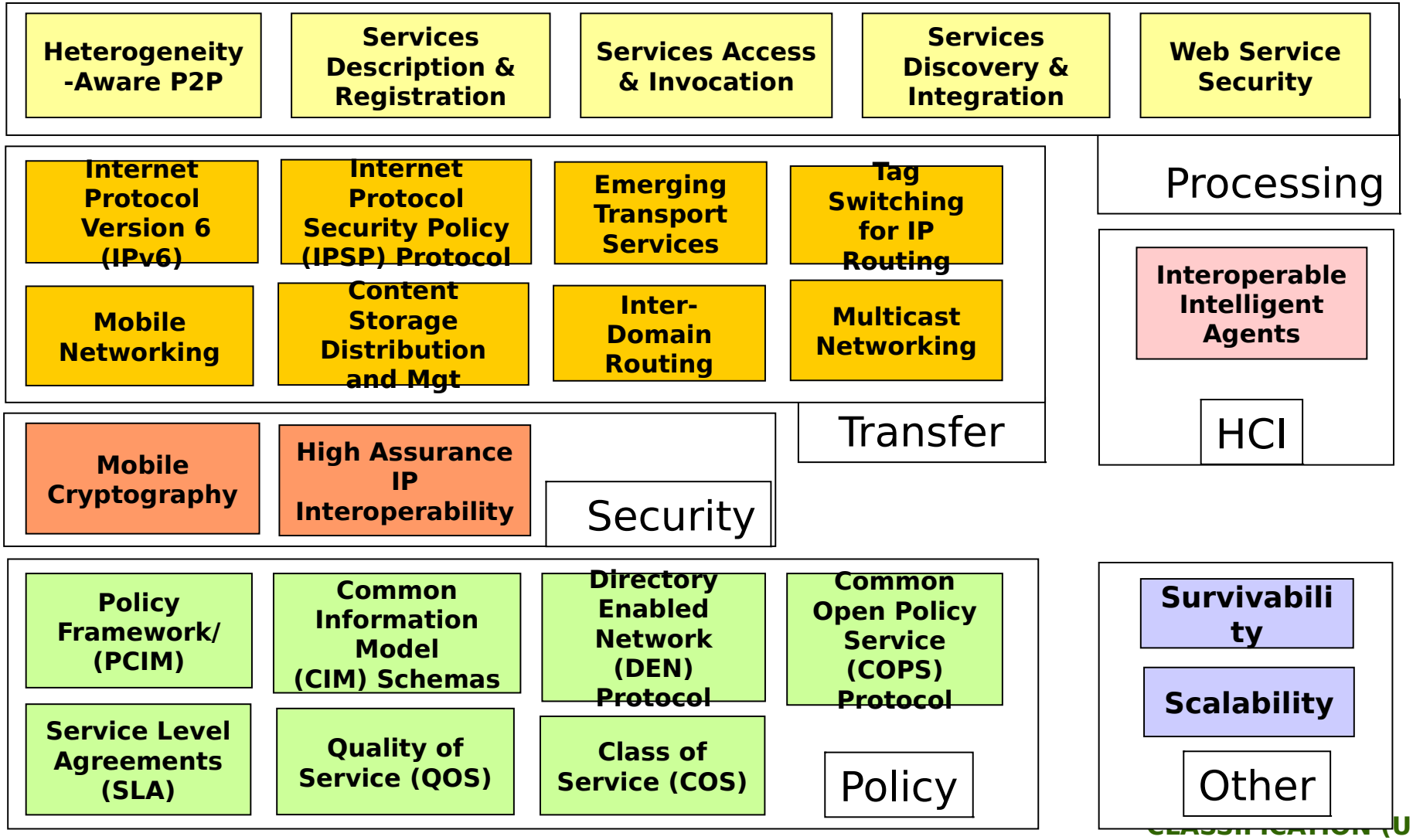
(NCOW) Reference Model


Provide Net-Centric Information Environment A0
Interact with Net-Centric Services A1
Perform Net-Centric User/Entity Services A2
Provide Net-Centric Services A3
Resource Service Requests A4
Manage Net-Centric Information Environment A5

(NCOW) Reference Model


Provide Net-Centric Services A3
Provide Core Services A31
Provide COI Services A32
Perform Environment Control Services A33
Provide Core Services A31
Perform Discovery Services A311
Provide Collaboration Services A312
Provide Messaging Services A313
Perform Information Mediation Services A314
Perform Information Storage Services A315
Provide Core Applications/ Functions A316

NCOW RM Target Technical View
(Technical Areas by Core IT Category)



NCOW RM Conformance and Compliance

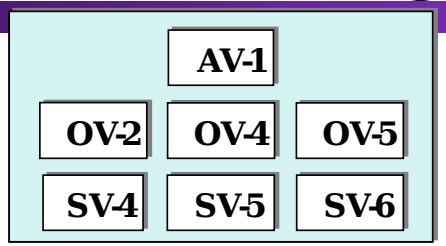
All DoD architectures are expected to comply and conform to the NCOW RM by:

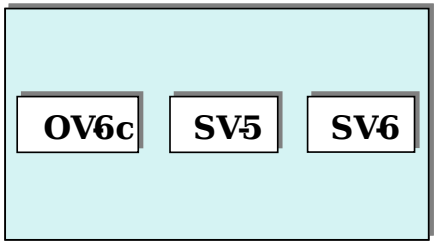
- Using common NCOW RM definitions and vocabulary
- Incorporating the capabilities and services described in the NCOW RM
- Incorporating the IT/NSS standards identified in the NCOW RM

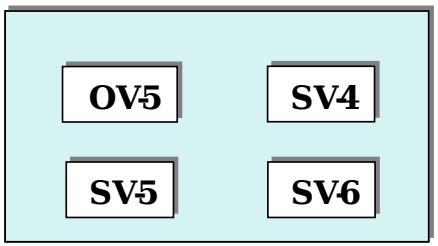
This supports Compliance and conformance with the GIG translates to satisfying the requirements of the following five products:

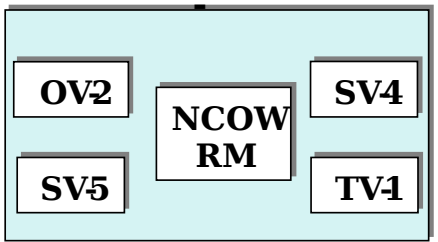
- DoD Architecture Framework (DoDAF)
- Net-Centric Operations and Warfare Reference Model (NCOW RM).
- Joint Technical Architecture (JTA) and the NCOW RM.
- Core Architecture Data Model (CADM).
- GIG Enterprise Services (GIG ES) Capability Description Document (CDD)

Integrated Architecture



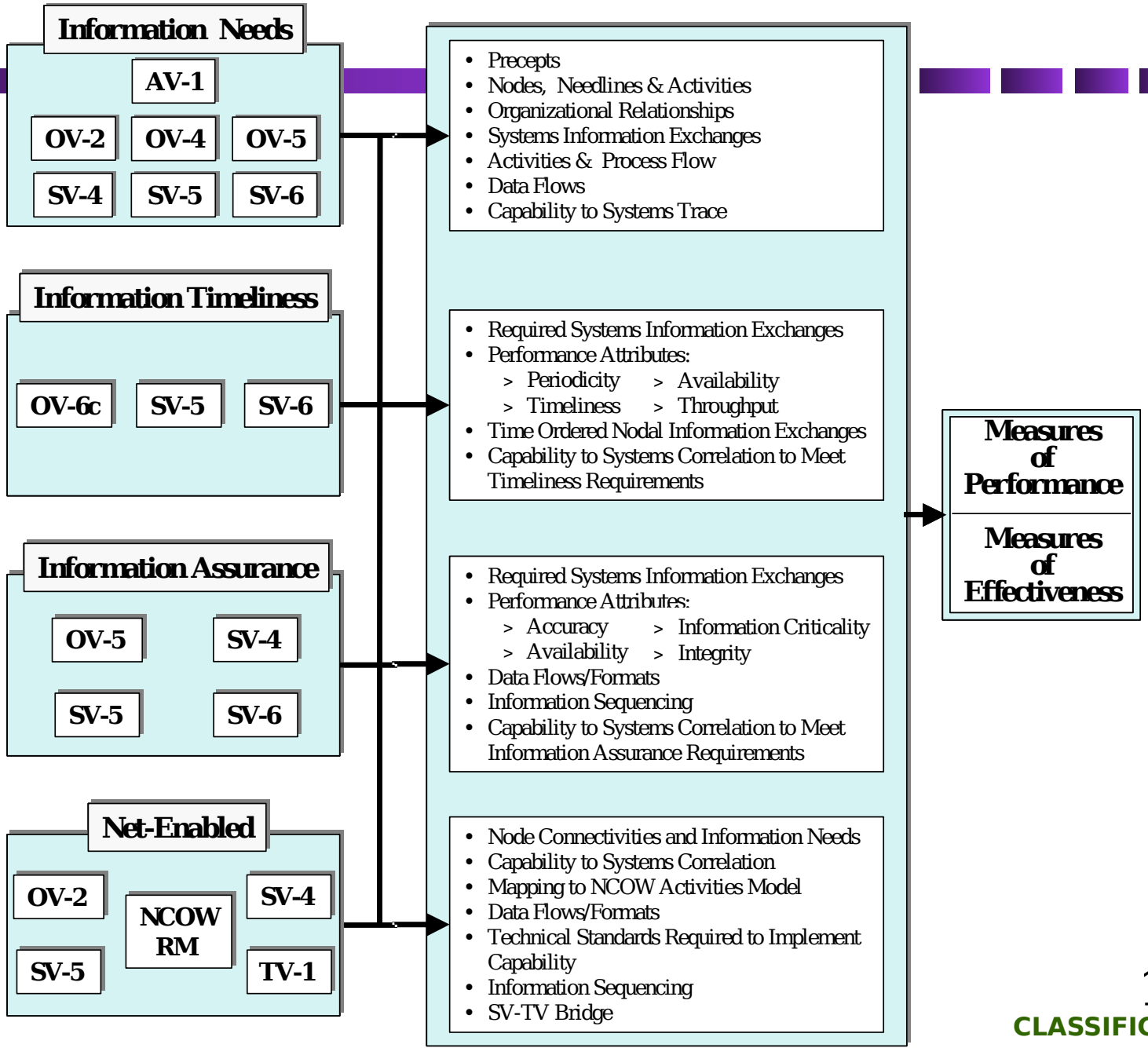






- **Operational Nodes**
- **Organizational Relationships**
- **Operational Activity**
- **Operational Event-Trace**
- **Systems Functionality Description**
- **Operational Activity to Systems Function**
- **Systems Data Exchange**
- **Technical Architecture Profile**

Integrated Architecture



Supporting Integrated Architecture Products

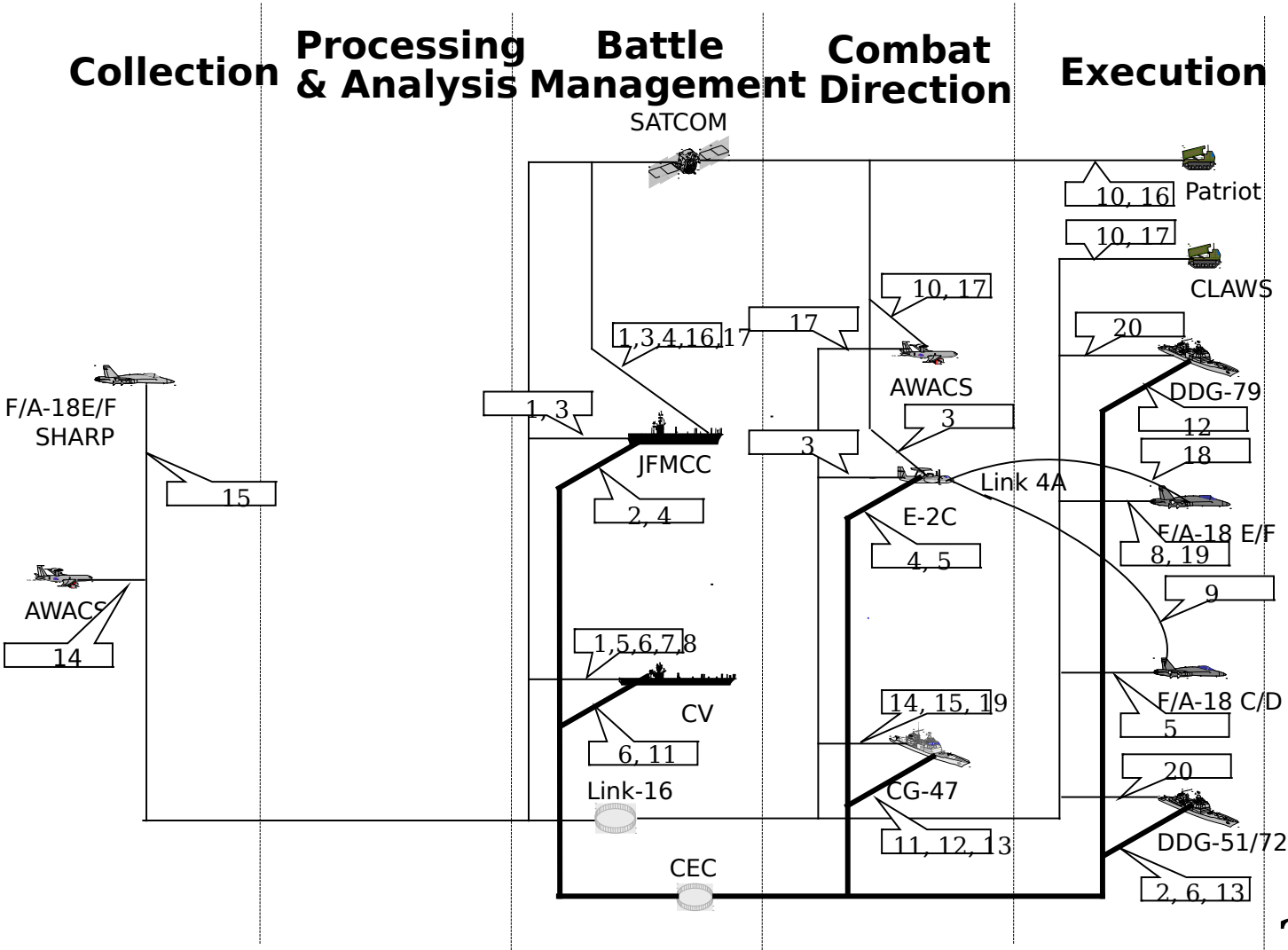
Framework Products	Framework Product Name	General Description
AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
OV-2	Operational Node Connectivity Description	Operational Nodes, operational activities performed at each node, connectivity and information exchange needlines between nodes
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
OV-5	Operational Activity Model	Operational activities, relationships among activities, inputs and outputs. Overlays can show cost performing nodes, or other pertinent information.
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity sequence and timing – traces actions in a scenario or sequence of events and specifies timing of events
SV-4	Systems Functionality Description	Functions performed by systems and the information flow among system functions
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to operational capabilities or of system functions back to operational activities.
SV-6	Systems Data Exchange Matrix	Provides details of systems data being exchanged between systems.
TV-1	Technical Standards Profile	Extraction of standards that apply to the given architecture.

Architecture Analysis

Focus on Architecture and Standards.

- **First order analysis - identifying capability gaps, shortfalls and duplications.**
- **Second order analysis - identifies interoperability requirements.**

SV-1: 2003 Strike Mission Node Connectivity Diagram



Note: Notional architecture for instructional purposes

Operational Activity to Systems Function Traceability Matrix (SV-5)

System Functions	Operational Activities															
	3.11	3.11.3	3.12	3.12.1	3.12.2	3.12.3	3.13	3.14	3.14.1	3.14.2	3.14.3	3.14.4	3.15	3.16	3.17	3.17.1
1	X															
1.1		X														
1.1.1			X													
1.1.1.1	X															
1.1.1.2					X											
1.1.1.3							X									
1.1.2										X						
1.1.2.1				X												
1.1.2.2						X										
1.1.2.3								X								
1.1.3											X					
1.1.3.1													X			
1.1.3.2									X							
1.1.3.3														X		
1.1.3.4														X		

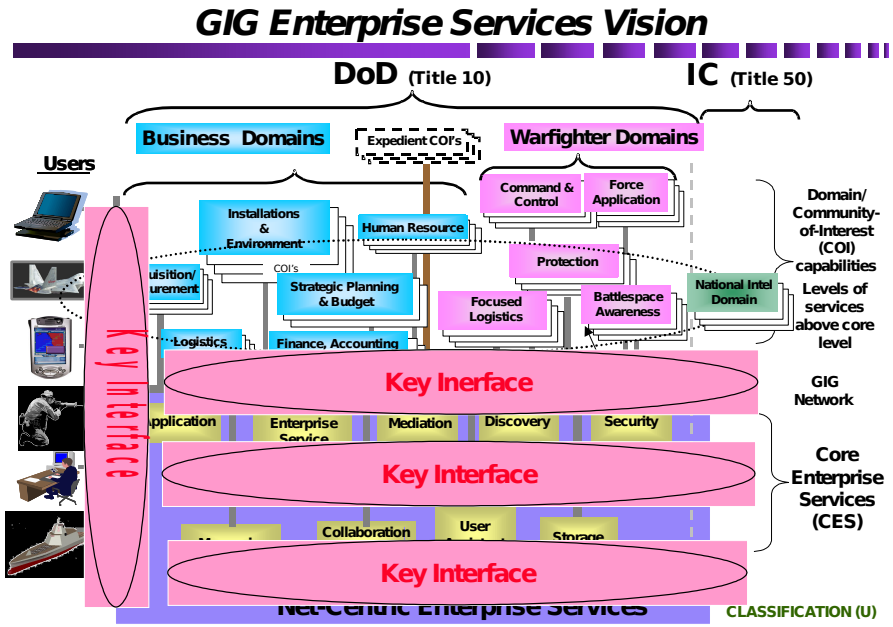
Systems Data Exchange Matrix (SV-6)

SV-6: 2003 Strike Mission (Illustrative Data)

IER No.	Sender	Receiver	Content	Media	Info Char	Format	Security	Freq	Timeliness	Thru put
1	JFMCC	CVIC	Target ID	JTIDS/SAT	Data	J 3.90	KGV-8	N/A	30 sec	N/A
2	DDG-51	JFMCC	Track Init.	DDS	Sensor	CEC data	KY-?	N/A	1 sec	N/A
3	JFMCC	E-2C	Engage Order	JTIDS/SAT	Data	J 13.85	KGV-8	N/A	15 sec	N/A
4	E-2C	JFMCC	Track Update	DDS	Sensor	CEC data	KY-?	N/A	7ms	N/A
5	CVIC	F/A-18	Engage Order	JTIDS	Data	J 13.85	KGV-8	N/A	10ms	N/A
6	DDG-51	CVIC	Target Loc	DDS	Sensor	CEC data	KY-?	N/A	4 sec	N/A
7	Patriot	CVIC	Target Acq	JTIDS	Data	J 4.56	KGV-8	N/A	2 min	N/A
8	F/A-18CD	CVIC	Target Killed	JTIDS	Data	J 8.76	KGV-8	N/A	3 min	N/A
9	E-2C	CVIC	CAP Posit	JTIDS	Data	J 10.74	KGV-8	N/A	35 sec	N/A
10	Patriot	AWACS	Target Loc	JTIDS/SAT	Data	J 12.101	KGV-8	N/A	4 Sec	N/A
11	CG-47	CVIC	Target Loc	DDS	Sensor	J 12.101	KY-?	N/A	2 sec	N/A
12	CG-47	DDG-81	Target ID	DDS	Sensor	CEC data	KY-?	N/A	1 sec	N/A
13	DDG-51	CG-47	Posit Info	DDS	Sensor	CEC data	KY-?	N/A	500 ms	N/A
14	CG-47	AWACS	Cse Orders	JTIDS	Data	J 7.99	KGV-8	N/A	2 min	N/A
15	CG-47	SHARPS	Cse Orders	JTIDS	Data	J 7.99	KGV-8	N/A	2 min	N/A
16	Patriot	JFMCC	Target Loc	JTIDS/SAT	Data	J 12.101	KGV-8	N/A	4 min	N/A
17	Hawk	JFMCC	Target Loc	JTIDS/SAT	Data	J 12.101	KGV-8	N/A	4 min	N/A
18	E-2C	F/A-18EF	Cse Orders	JTIDS	Data	FDL	KGV-8	N/A	30 sec	N/A
19	F/A-18EF	CG-47	Target ID	JTIDS	Data	J 3.90	KGV-8	N/A	30 sec	N/A
20	DDG-81	DDG-51	Target ID	JTIDS	Data	J 3.90	KGV-8	N/A	30 sec	N/A

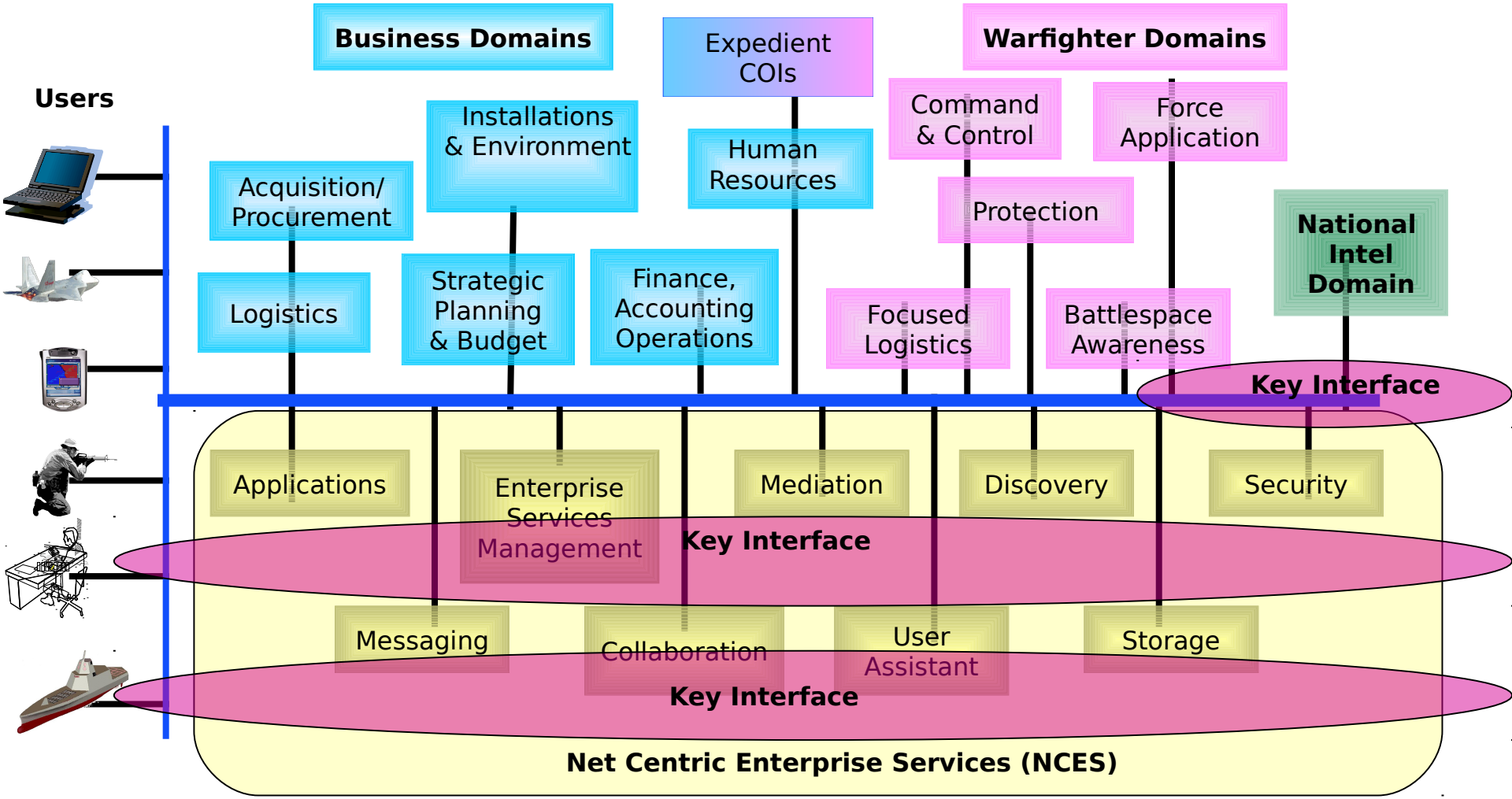
Note: Notional architecture for instructional purposes

Key Interface



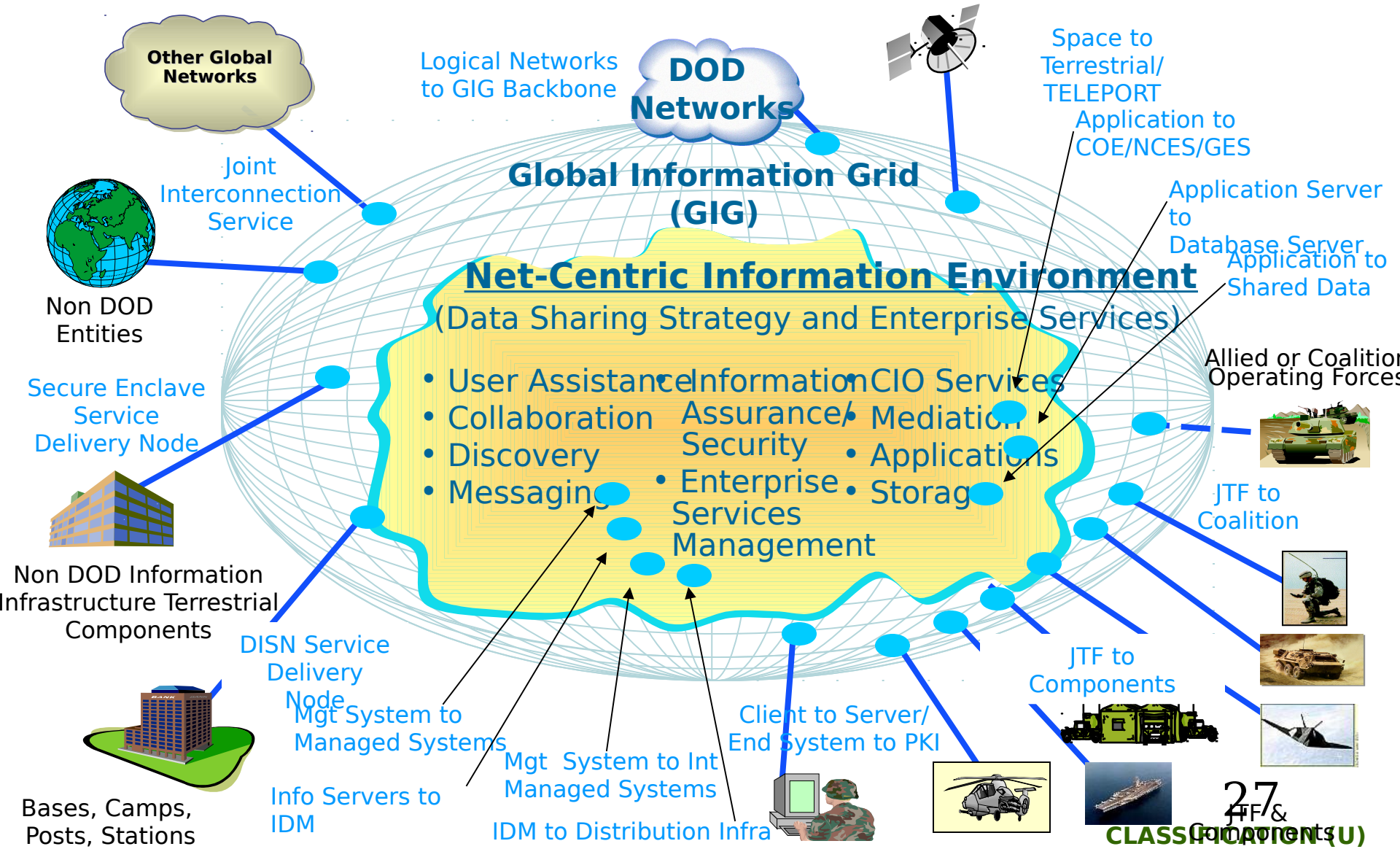
- **Organizational boundaries.**
- **Mission critical.**
- **Difficult or complex to manage.**
- **Capability, interoperability. or efficiency issues.**
- **Impacts multiple acquisition programs.**
- **Vulnerable**

GES/NCES



Key Interface

KIPs to NCES/GES



The 17 Key Interfaces

Communications KIPs

- Logical Networks to DISN Transport Backbone
- Space to Terrestrial Interface
- JTF to Coalition
- JTF Component to JTF Headquarters
- Teleport (i.e., deployed interface to DISN)
- Joint Interconnection Service
- DISN Service Delivery Node
- Secure Enclave Service Delivery Node (e.g., SCI/Collateral KIP)

Computing KIPs

- Application Server to Database Server
- Client to Server
- Applications to COE/CCP

Network Operations KIPs

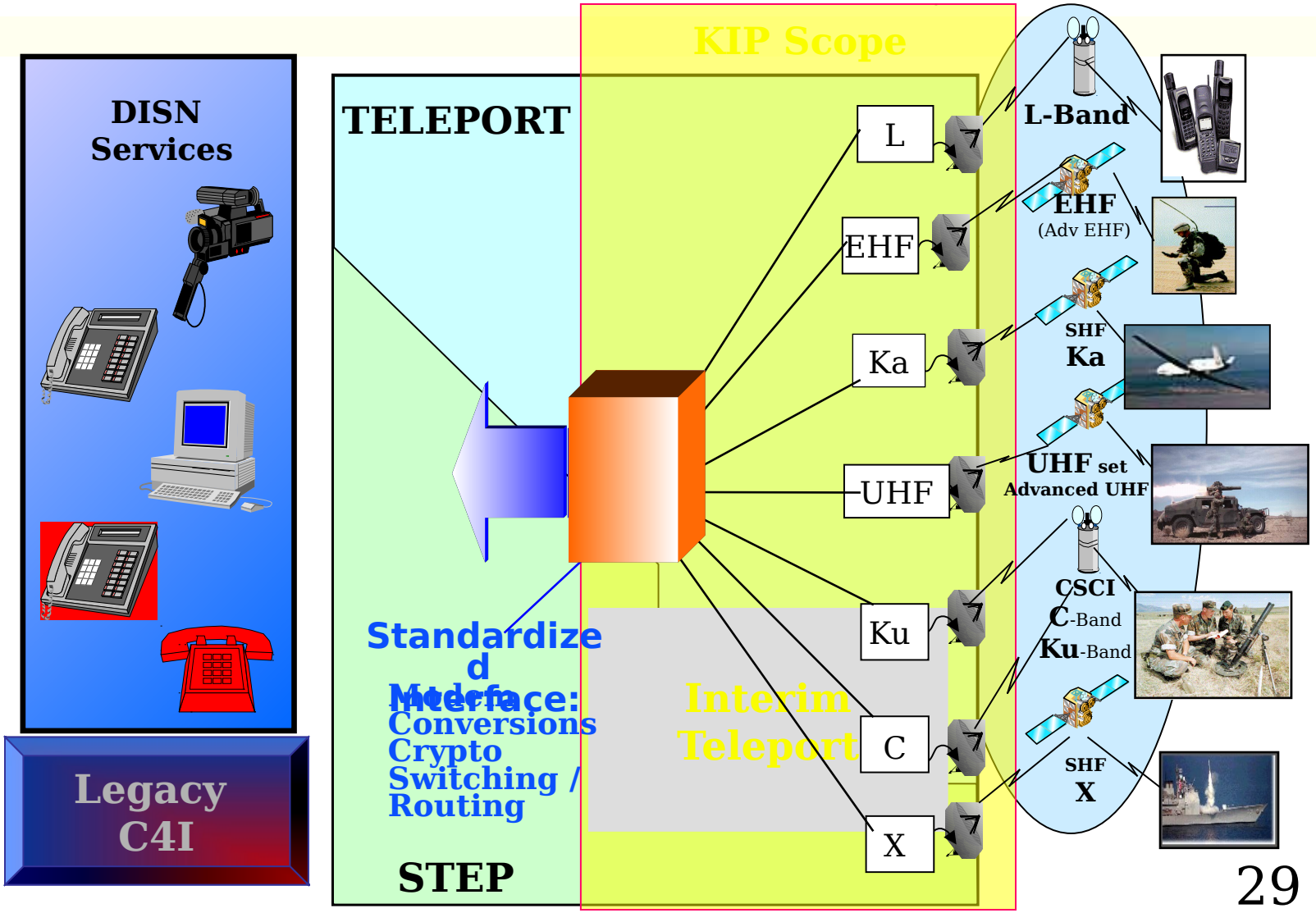
- End System to PKI
- Management Systems to (integrated) Management Systems
- Management Systems to Managed Systems
- IDM to Distribution Infrastructure
- Information Servers to IDM Infrastructure

Applications

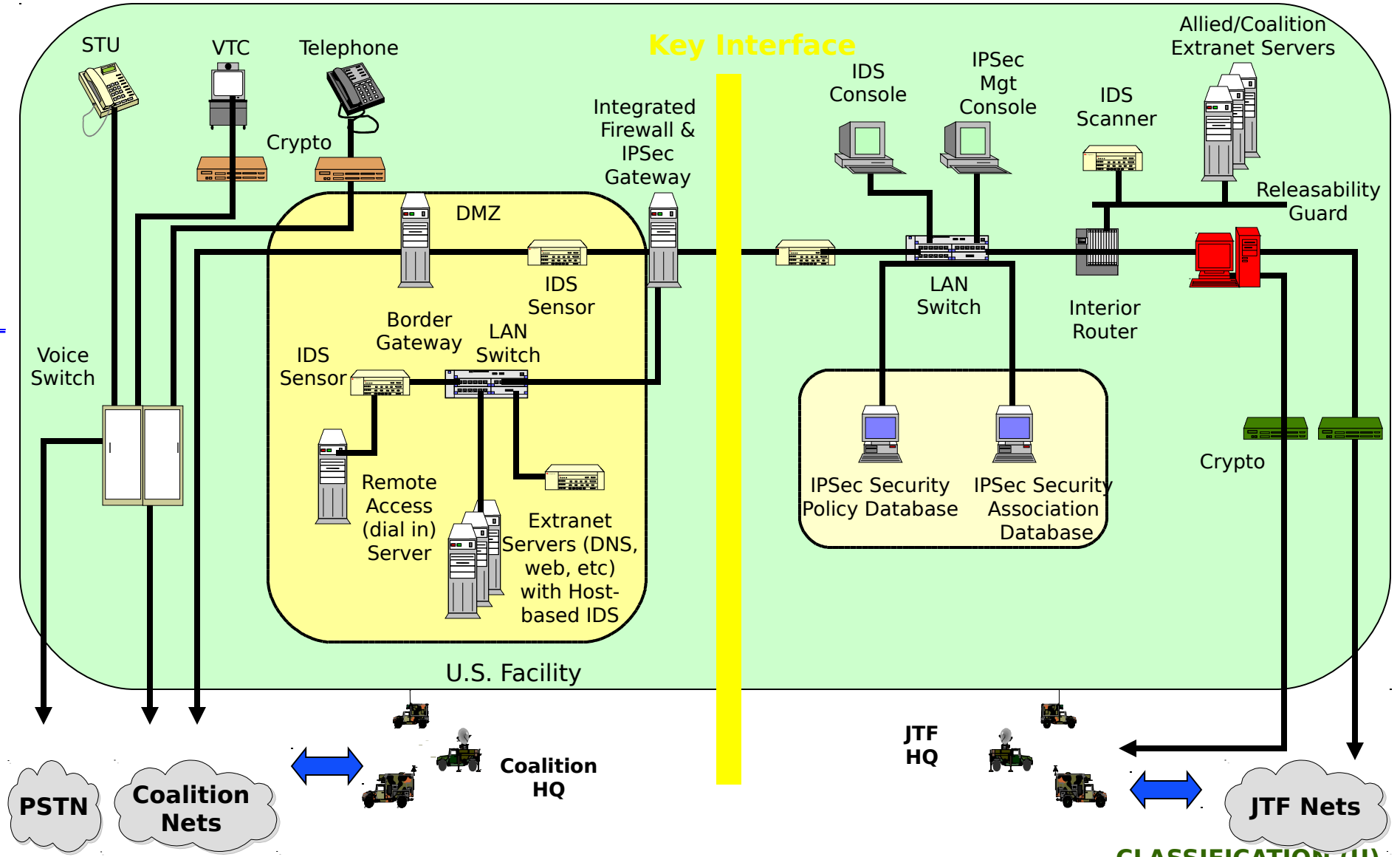
- Application Server to Shared Data (e.g., Situational Awareness Data KIP)

(Pilot Projects in Red)

STEP/TELEPORT



JTF to Coalition



Key Interface Profile

- ✓**Refined Operational View**
- ✓**Refined System View**
- ✓**Interface Control Specifications -- Interface Control Document (ICD)**
- ✓**Technical View & SV-TV Bridge**
- ✓**Configuration Management Plan**
- ✓**Procedures for Standards Conformance and Interoperability Testing utilizing reference implementations**
- ✓**Engineering Management Plan**

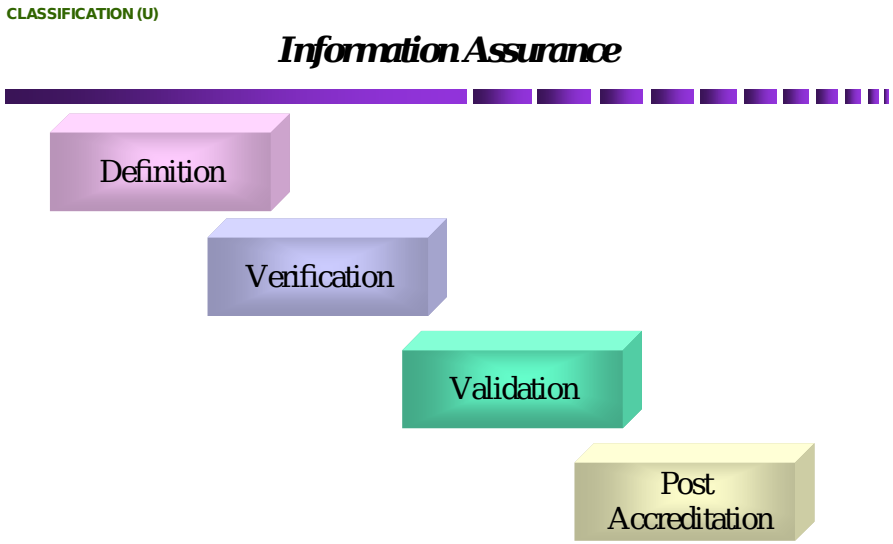
KIP Analysis

- **Logical Networks to DISN Transport Backbone.** Does your network connect to DISN Backbone?
- **Space to Terrestrial.** Does your ground terminal utilize or require access to DOD SATCOM programs such as DSCS, MILSTAR, FLTSAT, UFO, MUOS, Polar EHF, GPS, GBS, INMARSAT, Wideband Gapfiller, etc?
- **STEP and TELEPORT.** Does your ground terminal interface with/connect with STEP/TELEPORT systems?
- **JTF to Coalition.** Does your program or system interface with/connect the JTF to coalition forces?
- **JTF Component to JTF Headquarters.** Does your program or system interface/connect the JTF Component to the JTF Headquarters?
- **Joint Interconnection Service.** Does your organization connect the NIPRNET to Internet?
- **DISN Service Delivery Point.** Does your base, camp, post, station, unit or organization connect to the DISN?
- **Secure Enclave Service Delivery Point.** Does your system or program interface with or connect a Secure Enclave local area network to DISN service delivery point?
- **Client to Server.** Does your workstation publish, utilize or require access to data residing in DOD/NCES/GES servers?
- **End System to PKI.** Do your workstation and applications utilize or interface with utilize DOD **PKI?**
- **Information Servers to IDM Infrastructure.** Does your information server (collaboration, discovery, mediation, security, application, messaging, etc) require access to NCES/GES Infrastructure?
- **IDM to Distribution Infrastructure.** Does your network management system and communications system requires access to NCES/GES?
- **Management Systems to Managed Systems.** Does your system for personal and local computing manage the local network infrastructure (routers, WAPs, switches, hubs, firewalls, gateways, IDS), servers, and terminal devices (desktop computers, printers, wireless terminals?
- **Management Systems to (Integrated) Managed Systems.** Does your management system interface with DOD GNOSC, RNOSC? Includes NIPRNET NOC, GSSC, SIPRNET NOC, DSN NOC, DRSN NOC?
- **Applications Server to Database Server.** Does your web or application server require access to NCES/GES database server(s)?
- **Applications to Shared Data.** Does your application require access to shared data residing in NCES/GES infrastructure?
- **Application to COE/NCES/GES.** Does your application require access to COE/NCES/GES services?

KIP Compliance

- **Analysis required by PM to determine applicable KIPs**
- **Implemented IAW profile**
- **Validated during testing**

Information Assurance (DITSCAP)*



- **Availability**
- **Integrity**
- **Authentication**
- **Confidentiality**
- **Non-repudiation**

INFORMATION ASSURANCE (IA): **Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.**

*DoD Information Technology Security Certification and Accreditation Process

Certification and Accreditation Process (DITSCAP)

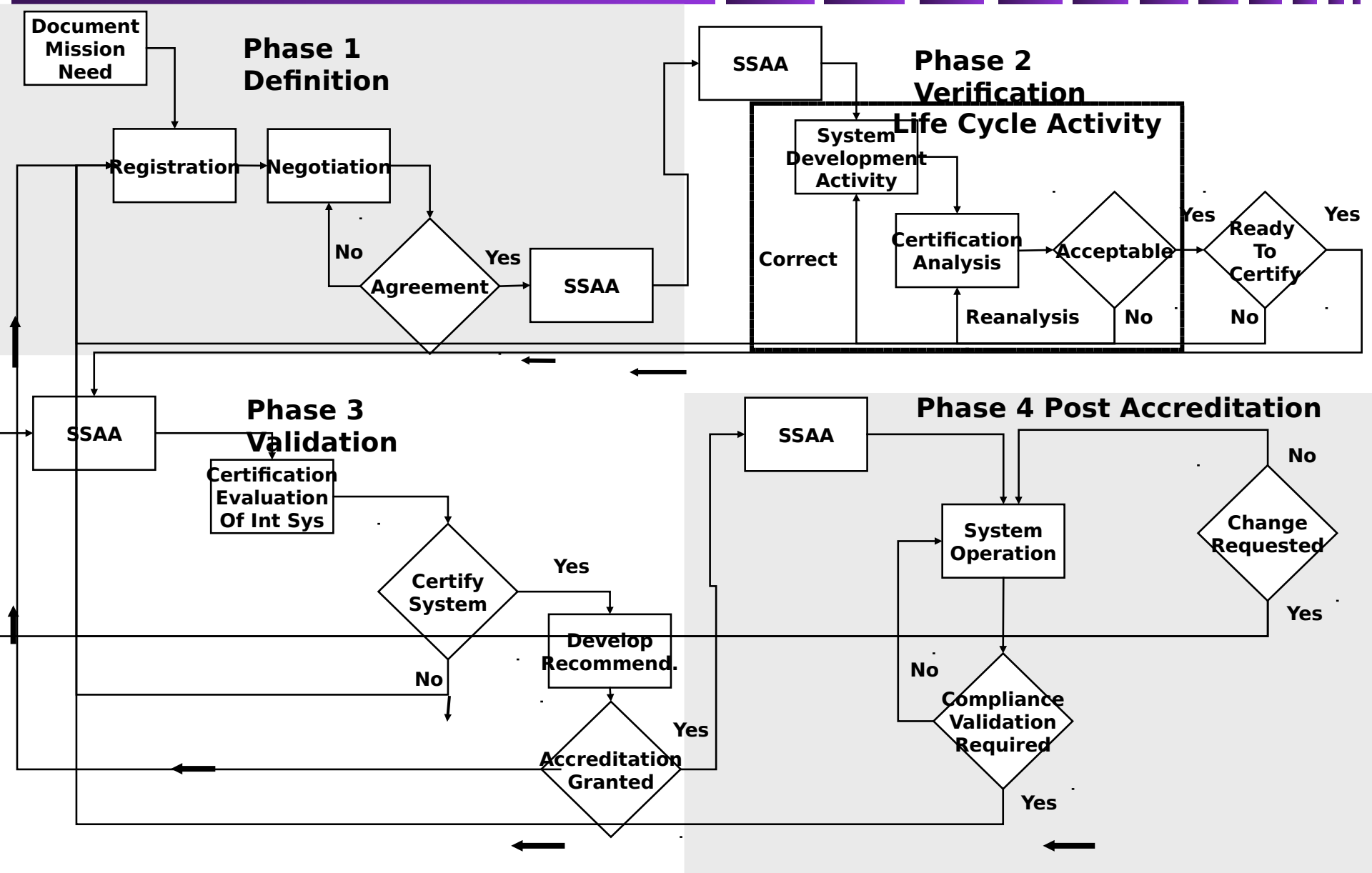


Table E4-1. Management Responsibilities by DITSCAP Phase.

Phase	Program Manager	DAA and CA	User Representative
Phase 1	Initiate security dialogue with DAA, the CA, and the user representative. Define system schedule and budget. Define and/or validate system performance, availability, and functionality requirements. Support DITSCAP tailoring and level of effort determination. Draft or support drafting of the SSAA. Reach agreement on the SSAA. Approve the SSAA.	Define ITSEC accreditation requirements. Obtain threat assessment. Begin vulnerability and risk assessments. Assign the CA. Support DITSCAP tailoring and determine the level of effort. Draft or support drafting of the SSAA. Reach agreement on the SSAA. Approve the SSAA.	Validate and/or define system performance, availability and functionality requirements. Support DITSCAP tailoring and level of effort determination. Reach agreement on the SSAA. Approve the SSAA.
Phase 2	Review the SSAA. Develop system or system modifications. Support certification actions. Review certification results. Revise system as applicable.	Review the SSAA. Evaluate developing system. CA performs certification actions. CA assesses vulnerabilities. CA reports results to the program manager, the DAA, and the user representative. Maintain the SSAA.	Review the SSAA. Support certification actions. Support certification actions.

Table E4-1. Management Responsibilities by DITSCAP Phase.

Phase	Program Manager	DAA and CA	User Representative
Phase 3	Review the SSAA. Test integrated system. Support certification actions. Review certification results. Revise system as applicable. Support SSAA revisions.	Review the SSAA. Evaluate developing system. CA performs certification actions. Assess vulnerabilities and residual risk. CA reports results to the program manager, the DAA, and the user representative. CA develops recommendation to the DAA. CA prepares accreditation package. Review the SSAA. Issue decision.	Review the SSAA. Support certification actions. Review certification results. Support SSAA revisions.
Phase 4	Review SSAA periodically. Operate system as described in the SSAA. Maintain an acceptable level of residual risk. Submit proposed changes to the user representative, the ISSO, the DAA, and the CA, as applicable. Support compliance validation.	Review the SSAA. Review proposed changes Oversee compliance validation.	Review the SSAA. Oversee system operation as described in the SSAA. Maintain an acceptable level of residual risk. Continuously review threat, system vulnerabilities and residual risk. Review and approve proposed changes. Submit significant changes to the DAA and the CA. Perform compliance validation actions.

Net Ready KPP Statement

Net Ready KPP	Threshold (T)	Objective (O)
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	100% of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements designated as enterprise-level or critical in the Joint integrated architecture	100% of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements in the Joint integrated architecture

Complementary and Corresponding Systems

- **GIG BE**
- **JTRS**
- **GCCS**
- **NCES**
- **TCS**
- **Crypto Modernization**
- **Collaboration Tools**
- **Horizontal Fusion**

Questions?

BACKUPS

Enforcement

- **If a program/system fails to meet certification requirements, the J-6 will not validate the program and will recommend the program not proceed to the next milestone and that funding be withheld until compliance is achieved and the program/system is validated. The J-6 will make this recommendation to the USD (AT&L), USD (P), USD (C), ASD (NII), the MCEB, and the JROC. The J-6 will also request that the program/system be added to the DOD 4630.8, Interoperability Watch List (IWL).**